U.S. Department of Justice

United States Attorney
Southern District of New York

The Silvio J. Mollo Building
One Saint Andrew's Plaza
New York, New York 10007

December 23, 2005

BY FACSIMILE

The Honorable Kenneth M. Karas
United States District Judge
Southern District of New York
Daniel Patrick Moynihan United States Courthouse
500 Pearl Street, Room 920
New York, New York 10007

Re: United States. v. Alberto William Vilar and Gary Alan Tanaka,
S1 05 Cr. 621 (KMK)

Dear Judge Karas:

The Government respectfully submits this letter in opposition to defendant Alberto Vilar's December 13, 2005 letter motion requesting that the Court order the Government to provide a list of search terms to govern the search of computers seized from the Amerindo U.S. office pursuant to a search warrant.

Background

On May 25, 2005, United States Postal Inspector Cynthia M. Fraterrigo applied for a warrant to search the offices of Amerindo U.S. located at 399 Park Avenue, New York, New York. In support of that application, Inspector Fraterrigo submitted an affidavit that stated, *inter alia*:

> 10. Based on my experience and on conversations with other law enforcement agents, I believe that it may be necessary that certain computer equipment, including input/output peripheral devices, keyboards, magnetic storage devices, related instructions in the form of manuals and notes, as well as the software utilized to operate such computers, be seized and subsequently processed by a qualified computer specialist in a laboratory setting, for the following reasons:
>
> a. Computer storage devices (such as hard disks, diskettes, compact disks, tapes, etc.) can store the equivalent of thousands of pages of information. In addition, a user may seek to conceal evidence of criminal activity

> by storing it in random order with deceptive file names. Searching authorities are thus required to examine all the stored data to determine which particular files are evidence or instrumentalities of criminal activity. This sorting process can take weeks or months, depending upon the volume of data stored, and it would be impractical to attempt this kind of data analysis "on-site" at the time of the execution of the search.
>
> . . . .
>
> f. The analysis of electronically stored data, whether performed on-site or in a laboratory or other controlled environment, may entail any or all of several different techniques. Such techniques may include, but shall not be limited to, surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files); "opening" or reading the first few "pages" of such files in order to determine their precise contents; "scanning" storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; and performing electronic "key-word" searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are related to the subject matter of the investigation.[1]

The Honorable Frank Maas signed the search warrant sought by Inspector Fraterrigo after making clarifying and grammatical modifications to the contents of the affidavit, and after adding language to the warrant requiring that the Government return any seized computers within ten days unless the Government received authorization from the Court to retain any such computer for a longer period of time. The warrant signed by Magistrate Maas authorized the Government to seize, among other things:

> Computers, hard drives, and any other devices or equipments [sic] capable of storing data or text in any format, including but not limited to cellular telephones, personal digital assistants, and any other storage media capable of containing data or text in magnetic, electronic, optical, digital, analog, or any other format, used to store information described above, as well as drafts and final versions of documents and correspondence prepared in connection with the running and supervision of the operations of the investment advisory business.

Argument

---

[1] The search warrant and affidavit are attached to defendant Vilar's brief in support of his motion to support evidence and statements as Exhibits A and B, respectively. (The criminal complaints, which were incorporated by reference in the warrant affidavit, are attached to Vilar's brief as Exhibits C and D).

Vilar contends that the Government's search of the computers seized from Amerindo U.S. should be circumscribed after the fact by a Court order requiring that keyword searches be conducted to isolate potentially relevant materials, and that the Government be precluded from examining any computer data that does not contain the keywords proposed by the Government and approved by the Court. Vilar's arguments are without merit and should be rejected by the Court.

The Fourth Amendment requires that search warrants specify with particularity the objects of the search, not the method of search. As the Tenth Circuit stated in *United States* v. *Brooks*, 427 F.3d 1246, 1251 (10th Cir. 2005), in the context of a challenge to the search of a computer seized pursuant to a search warrant, "[t]his court has never required warrants to contain a particularized computer search strategy. We have simply held that officers must describe with particularity the *objects of their search*." *See United States* v. *Hill*, 322 F. Supp. 2d 1081, 1090-91 (C.D. Cal. 2004) (rejecting defendant's claim that a search of his computer should have been limited to certain files more likely to be associated with child pornography and finding that "[f]orcing police to limit their searches to files that the suspect has labeled in a particular way would be much like saying police may not seize a plastic bag containing a powdery white substance if it is labeled 'flour' or 'talcum powder.' There is no way to know what is in a file without examining its contents, just as there is no sure way of separating talcum from cocaine except by testing it.").[2]

The warrant approved by Judge Maas permitted the Government to seize certain computers at Amerindo to search for materials set forth with particularity in the warrant. The Fourth Amendment requires nothing more, and the authorities cited by Vilar are inapposite. Vilar seemingly cites *United States* v. *Hunter*, 13 F. Supp. 2d 574 (D. Vt. 1998) for the broad proposition that failure to require such limitations on the search of the seized computers would run afoul of the particularity requirement of the Fourth Amendment. *Hunter* does not reach so far, however. Indeed, as the court noted in *United States* v. *Lloyd*, No. 98 Cr. 529 (ILG), 1998 WL 846822 at *3 (E.D.N.Y. Oct. 5, 1998), "*Hunter* does not hold that the absence of a plan to review computer materials is a *per se* violation of the particularity clause."

In *Hunter*, the Government sought and obtained a warrant to search an attorney's office and to seize computers and digital evidence. Because of the special circumstances posed by

---

[2] Numerous courts have found that "[i]n any thorough search for documents, even seemingly innocuous records must be examined to determine whether they fall with[in] the category of items covered by the warrant. *United States* v. *Triumph Capital Group, Inc.*, 211 F.R.D. 31, 63 (D. Conn. 2002) (citing *Andresen* v. *Maryland*, 427 U.S. 463, 482 n.11 (1976); *United States* v. *Ochs*, 595 F.2d 1247, 1248 (2d Cir. 1979). As the Court in *Triumph Capital Group* noted, "[f]ew people keep documents of their criminal transactions in a folder marked 'crime records'." *Id.*

searching an attorney's office, and the wealth of potentially privileged information to which those seizing and analyzing evidence would likely be exposed, the Government proposed a plan which was included in the warrant application "to ensure that all relevant computer records were retrieved without undue intrusion into records beyond the scope of the search." *Id*. at 584. The warrant itself, however, included the subsequent search limitations only with respect to certain digital storage devices, but not others. *Id*. After finding that "[c]omputer records searches are no less constitutional than searches of physical records, where innocuous documents may be scanned to ascertain their relevancy," *id*., the Court in *Hunter* held that materials seized pursuant to a paragraph of the warrant to which the limitations had not been incorporated had been taken in violation of the particularity requirement of the Fourth Amendment." *Id*. The Court went on, however, to find that the "good faith" exception established in *United States* v. *Leon*, 468 U.S. 897 (1984) applied, and that no suppression of evidence was warranted. *Id*. at 584-85.

Here, the Government was not bound by the terms of the warrant to conduct its search of seized electronic data according to a court-approved protocol as it was in *Hunter*. Rather, the warrant affidavit provided the Magistrate with a non-exclusive list of examples of the ways in which the Government would seek to locate the documents it sought to seize. Moreover, the special circumstance of *Hunter* – the search of an attorney's office which was apparently the impetus for including such a search protocol in the warrant – is not present here. In these circumstances, the warrant was sufficiently particularized, and the Government's search of the seized data through the means described in the warrant affidavit, is appropriate. Neither the warrant nor the caselaw cited by Vilar require anything more.

The other case cited by Vilar, *In re Grand Jury Subpoena Duces Tecum*, 846 F. Supp. 11 (S.D.N.Y. 1994) also is readily distinguishable. First, that case involved a motion to quash an assertedly overbroad grand jury subpoena, not the particularity of a search warrant approved by a Magistrate. Second, in that case, the subpoena called for the production of "the central processing unit (including the hard drive) of any computer supplied by X Corporation for the use of specified officers and employees of X Corporation or their assistants." *Id*. at 12. The subpoena was "not framed in terms of specified categories of information," but rather "demand[ed] specific storage devices." *Id*. The Court did not decide the Fourth Amendment question posed, but rather quashed the subpoena pursuant to Fed. R. Crim. P. 17(c), ordered X Corporation to preserve the materials so that the grand jury could issue a narrowed subpoena, and indicated that such a subpoena could be appropriately narrowed by the use of key-word searching. *Id*. at 13-14.

Here, the warrant authorized the seizure of electronic storage devices used to store the materials defined in the preceding 17 paragraphs of the warrant and authorized the search of those devices to locate the materials described in those 17 paragraphs. The Magistrate did not require the Government to employ any particular methodology to isolate irrelevant materials. *In re Grand Jury Subpoena Duces Tecum* involved wholly different circumstances and does not command the result sought by Vilar.

Accordingly, for the reasons set forth above, the Government respectfully requests that the Court deny defendant's motion to require the Government to devise a search protocol to be approved by the Court before conducting any further search of the computer evidence seized pursuant to the search warrant executed at Amerindo U.S.

Respectfully submitted,

MICHAEL J. GARCIA
UNITED STATES ATTORNEY

By: /s/
Marc Litt
Assistant United States Attorney
(212) 637-2295

cc: Susan C. Wolfe, Esq. (By facsimile)